***Sygn. akt: I C 55/18***

# WYROK
## W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 21 grudnia 2018 r.

***Sąd Okręgowy w Olsztynie Wydział I Cywilny***

Przewodniczący: SSO Juliusz Ciejek

Protokolant: p.o. sekr. sąd. Anna Kosowska

po rozpoznaniu w dniu 11 grudnia 2018 r. w Olsztynie

na rozprawie

na sprawy z powództwa ***P. D. i I. D.***

przeciwko ***(...) Bankowi (...) S.A. z siedzibą w W.***

o ***zapłatę***

I. zasądza od pozwanego (...) Banku (...) S.A. z siedzibą w W. solidarnie na rzecz powodów P. D. i I. D. kwotę 97.210 (dziewięćdziesiąt siedem tysięcy dwieście dziesięć) zł z odsetkami ustawowymi za opóźnienie od dnia 26 września 2016 r. do dnia zapłaty,

II. zasądza od pozwanego solidarnie na rzecz powodów kwotę po 6.417 (sześć tysięcy czterysta siedemnaście) zł tytułem zwrotu kosztów procesu, w tym kwotę 5.417 (pięć tysięcy czterysta siedemnaście) zł tytułem zwrotu kosztów zastępstwa procesowego.

Sygn. akt I C 55/18

# UZASADNIENIE

Pozwem z dnia 19 stycznia 2018 r. ***I. D. i P. D.*** zastępowani przez profesjonalnego pełnomocnika w osobie radcy prawnego, wnieśli o zasądzenie na ich rzecz solidarnie od pozwanego (...) Banku (...) S.A. z siedzibą w W. kwoty 97.210 zł wraz z ustawowymi odsetkami za opóźnienie od dnia 26 września 2016 r. do dnia zapłaty. Powodowie wnieśli także o zasądzenie od pozwanego na ich rzecz solidarnie kosztów postępowania, w tym kosztów zastępstwa procesowego wg. norm przepisanych.

W uzasadnieniu pozwu wskazali, że w dniach 23-26 września 2016 r. na skutek przełamania zabezpieczeń bankowych pozwanego padli ofiarą ataku hackerskiego. W jego wyniku hakerzy podszywając się pod nich, zalogowali się do ich systemu bankowości elektronicznej i dokonali nieautoryzowanych przez nich transakcji płatniczych obciążających ich rachunek. Pozwany, mimo obowiązku nie dokonał w odpowiednim czasie dodatkowej weryfikacji przelewów przez swój system, mimo ich podejrzanego charakteru. Ponadto mimo późniejszego telefonicznego kontaktu celem ich autoryzacji, nie poinformował ich o zaborze ich zasobów finansowych przez osoby nieuprawnione. Dalej powodowie podnieśli, że zdeponowanie środków na rachunku bankowym i niewydanie przez nich zlecenia ich wypłaty oznacza dalsze zobowiązanie banku do przechowywania tychże środków i ich wypłatę w każdej chwili na ich żądnie. Mimo wezwania do dnia złożenia pozwu pozwany nie zwrócił im dochodzonej pozwem kwoty. Stąd w ich ocenie wytoczenie powództwa było konieczne. (k. 4-18)

W odpowiedzi na pozew z dnia 7 marca 2018 r. pozwany ***(...) Bank (...) S.A. z siedzibą w W.*** zastępowany przez profesjonalnego pełnomocnika w osobie radcy prawnego, wniósł o oddalenie powództwa w całości oraz o zasądzenie kosztów zastępstwa procesowego wg. norm przepisanych.

Pozwany zaznaczył, że jego system bankowości elektronicznej w dniu wykonywania przedmiotowych operacji działał prawidłowo i nie był poddany żadnym atakom hackerskim. Również stan jego zabezpieczeń był prawidłowy i skuteczny. Dalej podał, że w wyniku przeprowadzenia wewnętrznego postępowania i analizy wynika, że do realizacji przedmiotowych transakcji doszło nie w wyniku zainfekowania jego systemu, ale zainfekowania złośliwym oprogramowania stacji roboczej powoda, z której to logował się na jego stronę internetową. Kolejno wskazał, że do powyższego by nie doszło, gdyby powodowie zainstalowali na swoim urządzeniu legalne oprogramowanie i program antywirusowy oraz aktualizowali go, zgodnie z regulamin korzystania z usług elektronicznych. Jego zdaniem działania hakerów były możliwe, bowiem przez otworzenie przez powoda podejrzanego maila, zainstalowano oprogramowanie szpiegowskie, które zainfekowało komputer. Dalej pozwany podniósł zarzut przyczynienia się powoda w całości do powstania szkody. Powyższe przejawiało się niezachowaniem należytej staranności w ochronie swoich danych, co doprowadziło do ich udostępnienia osobom nieuprawnionym, co z kolei umożliwiło wykonanie wskazanych przez nich przelewów. Następnie podał, że zlecone operacje nie mogły zostać poddane jakimkolwiek dodatkowym weryfikacjom przez system banku, ponieważ nie istnieją żadne możliwości techniczne, aby każdy przelew składany w taki sposób, mógł być wychwycony przez system informatyczny, jako przelew składany przez osobę nieuprawnioną, gdyż użyte hasła i kody znane są tylko klientowi banku i to one są narzędziem autoryzacji. Zdaniem pozwanego banku, skoro po stronie powodów doszło do rażącego niedbalstwa w zakresie ochrony danych wymaganych do logowania do systemu transakcyjnego, to brak jest podstaw do przypisania mu odpowiedzialności za skradzione powodom środki finansowe. (k. 102-113, 200-203, 211-215, 232)

W pismach przygotowawczych powodowie wskazywali, iż pozwany w żaden sposób nie wykazał, aby którekolwiek z ich działań miały być umyśle lub też nosiły cechy rażącego niedbalstwa. Za takowe nie można uznać podanego przez powoda jednego numerów z karty kodów kreskowych do rachunku bankowego, skoro strona internetowa, na którą się logował była identyczna, jak strona pozwanego banku oraz pojawiały się na niej wiarygodne komunikaty. Także powód wówczas posiadał na swoim laptopie zabezpieczenie antywirusowe, dokonywał jego aktualizacji oraz regularnie go serwisował w salonie. Ponadto po telefonicznej rozmowie z pracownikami pozwanego dokonał – za ich sugestią – reinstalacji i przeformatowania dysku komputera, aby się pozbyć potencjalnego zagrożenia atakiem wirusów. W związku, z czym zdaniem powodów nie naruszyli oni żadnych postanowień umowy czy też regulaminu korzystania z usług elektronicznych. W ich ocenie to niewłaściwe działanie pozwanego banku doprowadziło do przejęcia środków z ich rachunku, albowiem w porę nie podjął on stosownych działań zapobiegających powyższemu. (k. 160-165)

***Sąd ustalił następujący stan faktyczny:***

W dniu 5 lutego 2014 r. I. D. i P. D. zawarli z (...) Bankiem (...) S.A. z siedzibą w W. umowę rachunku oszczędnościowo-rozliczeniowego (...) konta za zero, usług bankowości elektronicznej oraz karty debetowej (bez (...)). W ramach zawartej umowy bank utworzył dla nich rachunek oszczędnościowo-rozliczeniowy (tzw. (...)) o nr (...) oraz rachunek oszczędnościowy o nr (...). Klientom przy zwieraniu umowy udzielono informacji jak korzystać i wykonywać operacje bankowe za pośrednictwem elektronicznego sytemu bankowego. Natomiast nie udzielono im szczegółowych pouczeń, co do sprzętu za pomocą, którego mogli ich dokonywać, w tym jego zabezpieczenia, konserwacji oraz potencjalnych niebezpieczeństw, tj. ataki hackerskie. P. D. jedynie ogólnie wiedział, że musi zwracać uwagę na poziom bezpieczeństwa strony internetowej banku, na której miał się logować. Powyższe oznaczało, że strona taka winna być wyposażona w zieloną kłódkę i prefiks witryny „https". Pierwsze potwierdza, że strona posiada sprawdzony i ważny certyfikat, natomiast drugie, że jest ona szyfrowana. Te dwa elementy oznaczały, że połącznie ze stroną internetową (...) Banku (...) S.A. z siedzibą w W. jest bezpieczne i można na niej dokonywać operacji bankowych. Narzędziem, które małżonkowie D. wybrali do autoryzacji obsługi konta i zabezpieczające wykonywane przez nich operacje bankowych była karta kodów kreskowych, czyli kodów numerycznych z tzw. „zdrapki". Natomiast, jeśli chodzi o login i hasło do logowania na stronę internetową banku to znali je jedynie oni.

(dowód: umowa rachunku oszczędnościowo-rozliczeniowego (...) konto za zero, usług bankowości elektronicznej oraz karty debetowej (bez (...)) z dnia 5 lutego 2014 r. – k. 29-34, regulamin świadczenia usług bankowości elektronicznej w (...) Banku (...) S.A. z siedzibą w W. – k. 132-143, 188-195v, zeznania powoda – k. 323v-326)

W małżeństwie D. bankowością internatową, tj. wykonywaniem operacji i przelewów od 2010 r. – w ramach innych rachunków bankowych – zajmował się jedynie P. D.. Zawsze chwalił sobie ten rodzaj usług bankowych i nigdy nie miał z nimi żadnych problemów. Jeśli natomiast chodzi o jego małżonkę, to I. D. używała zazwyczaj jedynie karty płatniczej przypisanej do tych rachunków celem dokonywania płatności po zrobieniu przez nią zakupów. Przy korzystaniu z usług bankowości elektronicznych P. D. używał jedynie swojego prywatnego laptopa marki M. o nr seryjnym (...). Laptop ten wygrał na konkursie przeprowadzonym przez fundację (...) dla nauczycieli. Serwisował go regularnie w serwisie komputerowym (...) w O..

(dowód: zeznania powoda – k. 323v-326, zeznania powódki – k. 326, zaświadczenie z dnia 10 stycznia 2018 r. z serwisu komputerowego (...) dot. serwisowania laptopa powodów – k. 93)

W czwartek 22 września 2016 r. powód próbował zalogować się na swoje konto w serwisie internetowym (...) Banku (...) S.A. z siedzibą w W. celem wykonania przelewu na rzecz kościoła tytułem wyjazdu na tzw. rekolekcje dłuższe. Jak zawsze upewnił się, że połączenie jest bezpiecznie (zielona kłódka + element „https") i podając login i hasło oraz przepisując treść znajdującą się w okienku z obrazkiem, skutecznie zalogował na swoje konto. Po zalogowaniu mógł swobodnie poruszać się po serwisie internetowym, widział ostatnio dokonywane przez siebie operacje oraz stany swoich rachunków. Nic w działaniu strony ani jej wyglądzie nie budziło jego niepokoju. Chwilę po zalogowaniu na monitorze wyświetlił mu się komunikat, że z powodu „przebudowy" strony musi on podać kod nr 21 z karty zdrapki, albowiem w przeciwnym razie wykonanie przelewów w ciągu najbliższych 7 dni zostanie przez bank zablokowane. Komunikatu tego nie można było wyłączyć. Powód będąc w przekonaniu, że skoro poprawnie się zalogował i widzi stan rachunków oraz historię dokonywanych przez siebie przelewów jest na prawidłowej stronie banku, podał żądany kod. Po krótkim czasie strona się zawiesiła i nie można było na niej zrobić żadnej operacji. Pojawił się komunikat, że dostęp do serwisu jest czasowo niemożliwy. Wobec powyższego P. D. wylogował się ze strony banku. Powyższe nie wzbudziło w nim niepokoju. Stwierdził, bowiem, że skoro strona jest „w przebudowie" nastąpiła przerwa w dokonywaniu usług bankowych.

(dowód: protokół przyjęcia ustnego zawiadomienia o przestępstwie i przesłuchanie w charakterze świadka P. D. – 69-72, zeznania powoda – k. 323v-326)

Kilka dni przed powyższą próbą wejścia na swoje konto bankowe, P. D. na skrzynkę mailową, otrzymał wiadomość e-mail z informacją o otrzymaniu paczki. Po wejściu w wiadomość okazało się, że firma kurierska wzywała go do odbioru paczki, której nie zamawiał. Powyższe nie wzbudziło w nim żadnego podejrzenia. Stwierdził on, bowiem, że prawdopodobnie doszło do zwykłej pomyłki.

(dowód: zeznania powoda – k. 323v-326, karta zgłoszenia reklamacji nr (...) z dnia 3 października 2016 r. – k. 73, zeznania powoda – k. 323v-326)

W dniach 23-26 września 2016 r. w wyniku działań przestępczych o charakterze hackerskim, na w/w rachunkach powodów nastąpiły serie nieautoryzowanych przez nich standardowych przelewów E. oraz szybkich przelewów (...). Najpierw w dniu 23 września 2016 r. z rachunku oszczędnościowego powodów przelano na ich rachunek (...) kwotę 60.000 zł i tego samego dnia wytransferowano „na zewnątrz" kwotę 57.190 zł wykorzystując trzy przelewy na kwoty 18.410 zł, 19.290 zł i 19.490 zł. Następnie w dniu 26 września 2016 r. z tego samego rachunku oszczędnościowego przelano na rachunek (...) kwotę 50.000 zł i tego samego dnia wytransferowano również „na zewnątrz" kwotę 54.947 zł wykorzystując trzy przelewy na kwoty 19.490 zł, 18.610 zł i 16.847 zł. Zewnętrzne wytransferowanie środków odbyło się na konto przypisane D. J. o nr (...) w Banku (...) S.A. z siedzibą we W., a w tytule przelewów wpisano fikcyjne oznaczenia faktur VAT. Przelewy te były dokonywane standardowym przelewem E., przez które łącznie

wytransferowano z rachunków powodów kwotę 112.137 zł. Natomiast inne szybkie przelewy (...) wykonywane na rachunku powodów zostały przez bank wychwycone i zablokowane.

(dowód: zestawienie operacji na rachunkach bankowych powodów – k. 35-36, wyciąg z logów systemowych transakcji, operacji i czynności wykonywanych na koncie powodów – k. 157-159, 196-198)

W tym okresie czasu, tj. od następnego dnia po nieudanej próbie logowania do dnia 28 września 2016 r (środa) powód nie logował się na stronę banku i nie korzystał z bankowości elektronicznej. Również od dnia 17 września 2016 r. (niedziela) nie korzystał on z telefonu komórkowego, ponieważ przez przypadek zostawił go w samochodzie, którym jechał dzień wcześniej na wesele do swoich bliskich. Telefon odnalazł się dopiero w dniu 28 września 2016 r. (środa), kiedy to oddał go mu jego szwagier, który znalazł go pod siedzeniem swojego samochodu, którym wspólnie z powodem jechali na ślub. Telefon był całkowicie rozładowany. Po jego podładowaniu i uruchomieniu nie sygnalizował on jakichkolwiek prób wcześniejszych połączeń do powoda od innych osób - nie przyszły, bowiem jak zwykle żadne wiadomości – powiadomienia sms o próbie kontaktu przez kogokolwiek.

(dowód: zeznania powoda – k. 323v-326, zeznania powódki – k. 326)

W dniu 28 września 2016 r. (czwartek) telefonicznie najpierw z powódką, a następnie czterokrotnie z powodem skontaktowali się pracownicy pozwanego z (...) Banku (...) S.A. z siedzibą w W.. W trakcie rozmów wyjaśniali, że dzwonią w celu potwierdzenia (autoryzowania), – choć tak naprawdę w celu weryfikacji – przelewów na znaczne kwoty, które mają być realizowane z konta powodów na konto D. J.. P. D. odmówił ich potwierdzeń oraz zażądał zablokowania konta. Pracownicy banku natomiast prosił go o niekorzystanie z karty kodów numerycznych ze zdrapki. W trakcie dalszej rozmowy jeden z pracowników banku zasugerował, że być może P. D. otwierał maile z jakimiś podejrzanymi wiadomościami i dołączonymi do nich załącznikami. Po zastanowieniu powód przyznał, że otrzymał jednego maila z informacją od kuriera o odbiorze paczki. Jednakże podał, że wiadomość ta nie była skierowana do niego, albowiem nie zamawiał żadnej paczki. Wobec powyższego wskazał, że wówczas wiadomość ta nie wzbudzała w nim niepokoju, albowiem stwierdził on, że była to zwykła pomyłka. Pracownik banku zasugerował, zatem, żeby powód sprawdził, czy na jego komputerze nie ma wirusa i jeśli go znajdzie, żeby oddał go do serwisu celem reinstalacji i przeformatowania dysku. Podczas tych rozmów żaden z pracowników banku nie poinformował natomiast powodów o zaborze środków z ich rachunku bankowego – mimo wiedzy o tym już w tamtej chwili. Wobec czego powodowie uznali, że doszło jedynie do próby włamania się na ich rachunek bankowy, natomiast zablokowanie konta oraz karty kodów w pełni zabezpieczy środki pieniężne na nim się znajdujące. Uznając, że sprawa jest zakończona, nie dokonali sprawdzenia stanu swoich rachunków na koncie bankowym.

(dowód: protokół przyjęcia ustnego zawiadomienia o przestępstwie z dnia 3 października 2016 r i przesłuchanie w charakterze świadka powoda P. D. - k. 69-72, zeznania powoda – k. 323v-326 , nagrania CD z 4 rozmów telefonicznych pracowników pozwanego z powodem – k. 206, 224, 240-244, zeznania świadka P. C. – k. 205v-207v, wykaz połączeń – k. 240-244)

W następnym dniu, tj. 29 września 2016 r. P. D., zgodnie z sugestiami pracownika pozwanego zaniósł sprzęt do serwisu celem reinstalacji systemu operacyjnego. Powyższe zatarło wiele informacji z działań dokonywanych na tym laptopie. W chwili obecnej nie jest już możliwe rozstrzygnięcie czy komputer powoda został zawirusowany złośliwym oprogramowaniem lub oprogramowaniem wyłudzającym dane. Obecnie nie można także jednoznacznie określić, jaki system operacyjny był zainstalowany przed tą datą na laptopie powoda oraz czy był on systemem legalnym, jak też czy posiadał program antywirusowy. Z informacji, jakie zachowały się na dysku, wynika, że był to system z rodziny W.. Nie da się natomiast określić, jaka konkretnie wersja systemu była zainstalowana.

(dowód: zeznania powoda – k. 323v-326, opinia biegłego sądowego K. D. – k. 268-273, ustana uzupełniająca opinia biegłego sądowego K. D. – k. 322-323, opinia biegłego sądowego K. D. wydana w postępowaniu przygotowawczym – k. 83-92)

W dniu 29 września 2016 r. (...) Bank (...) S.A. z siedzibą w W. sporządził zawiadomienie o podejrzeniu popełniania przestępstwa oraz pismem z dnia 17 października 2016 r. uzupełnił to zawiadomienie. W ich treści wskazał m. in., że zidentyfikował on przypadki realizacji nieuprawnionych przelewów z rachunków powodów dokonanych jego zdaniem poprzez prawdopodobnie zainfekowany złośliwym oprogramowaniem komputer. Powyższe informacje podał, mimo, że żaden z jego pracowników nie zbadał laptopa powodów. Dalej wskazał, że środki te zostały początkowo zaksięgowane na rachunku należącym do D. J. i następnie wytransferowane na inne rachunki. Część środków zostało przetransferowane za pośrednictwem kanału B. M. na kwotę 14.927 zł na konto prowadzone przez (...) Banku (...) S.A. z siedzibą w W. na rzecz S. C. (1). Wobec czego zgodnie z art. 106a ust. 3 i 4 Prawa bankowego w dniu 17 października 2016 r. o godz. 8:00 na 72 godziny na rachunku nr (...) założył blokadę środków na kwotę 14.920,10 zł. Ponadto bank zgodnie z art. 106c ust 5 i 6 Prawa bankowego zwrócił się o wydanie postanowienia prze uprawniony organ o przedłużenie tej blokady na dalszy okres 3 miesięcy.

(dowód: zawiadomienie z dnia 29 września 2016 r. o podejrzeniu popełnieniu przestępstwa – k. 41-46, zestawienie operacji z rachunków powodów – k. 47-48, 157-159, powtórny wydruk potwierdzenia wykonania przelewu z rachunku bankowego powodów – k. 49-50, uzupełnienie zawiadomienia o popełnieniu przestępstwa z dnia 17 października 2016 r. – k. 37-40)

W dniu 3 października 2016 r. (poniedziałek) powódka I. D. udała się osobiście do Oddziału 3 (...) Banku (...) S.A. z siedzibą w W., aby odblokować konto bankowe. W placówce okazało się, że nie zostało ono w ogóle zablokowane, pomimo wyraźnej dyspozycji telefonicznej jej męża - powoda. Dopiero podczas wizyty w banku (...) dowiedziała się, że przelewy, których P. D. telefonicznie nie autoryzował zostały wykonane oraz że z ich rachunków zniknęły pieniądze. W związku z tym od razu złożyła reklamację w tym przedmiocie, która to nie została przez bank uwzględniona.

(dowód: karta zgłoszenia reklamacji nr (...) z dnia 3 października 2016 r. – k. 73, zeznania powoda – k. 323v-326)

Po zgorszeniu reklamacji powód w tym samym dniu, tj. 3 października 2016 r. złożył ustne zawiadomienie o popełnieniu przestępstwa i został przesłuchany. Powódka zaś została przesłuchana w tej samej sprawie w dniu 28 listopada 2016 r.

(dowód: protokół przyjęcia ustnego zawiadomienia o przestępstwie z dnia 3 października 2016 r i przesłuchanie w charakterze świadka powoda P. D. - k. 69-72, protokół przesłuchania powódki I. D. z dnia 28 listopada 2016 r. –k. 74-75)

Prokuratura Rejonowa W. Ż. w W. w dniu 17 października 2016 r. wszczęła śledztwo w sprawie o sygn. akt PR 3 Ds. (...).2016.VI, m.in. w sprawie dokonania w krótkich odstępach czasu z góry powziętym zamiarem w celu osiągniecia korzyści majątkowej w okresie od 23 września 2016 r. do 28 września 2016 r. w bliżej nieustalonym miejscu nieuprawnionych transakcji za pośrednictwem sieci internet poprzez wykonanie bezprawnych przelewów środków pieniężnych na szkodę P. D. i I. D.. Postępowanie w zakresie tego czynu następnie prowadziła Prokuratura Rejonowa w Pile, zaś obecnie Prokuratura Okręgowa w Białymstoku.

(dowód: postanowienie o wszczęciu śledztwa z dnia 17 października 2016 r. – k. 53-56, zawiadomienie powoda o wszczęciu śledztwa – k. 63, zawiadomienie pozwanego o wszczęciu śledztwa – k. 65, pismo Prokuratury Rejonowej W. Ż. w W. z dnia 9 kwietnia 2018 r. – k. 181, pismo Prokuratury Okręgowej w Białymstoku z dnia 25 maja 2018 r. – k. 228-229)

Prokurator Prokuratury Rejonowej W. Ż., mając na uwadze wniosek banku, postanowieniem z dnia 17 października 2016 r. postanowił dokonać blokady rachunku bankowego o nr (...) prowadzonego przez (...) Bank (...) S.A. z siedzibą w W. dla S. C. (2) dotyczącą środków pieniężnych w wysokości 14.920,10 zł.

(dowód: postanowienie z dnia 10 stycznia 2017 r. o blokadzie środków na rachunku bankowym powodów – k. 67-68, zeznania powoda – k. 323v-326 )

Mając na uwadze dokonane w toku postępowania przygotowawczego ustalenia, w tym zwłaszcza zeznania świadków – P. D., S. C. (2) oraz P. C. Prokurator Prokuratury Rejonowej w Pile postanowieniem z dnia 10 stycznia 2017 r. uchylił powyższą blokadę. Ponadto uznał, że zatrzymane środki pieniężne w wysokości 14.927 zł stanowią własność P. D. i I. D. i jako zbędne dla postępowania karnego przekazał na ich rachunek prowadzony w pozwanym banku o numerze (...).

(dowód: postanowienie z dnia 10 stycznia 2017 r. o blokadzie środków na rachunku bankowym powodów – k. 67-68, zeznania powoda – k. 323v-326 )

Ostatecznie powodowie w dniu 15 grudnia 2017 r. wezwali pozwany bank do zwrotu ich środków pieniężnych w kwocie 97.210 zł wraz z należnymi odsetkami od dnia 26 września 2016 r. do dnia zapłaty, pod rygorem skierowania sprawy na drogę postępowania sądowego. W piśmie z dnia 2 marca 2018 r. pozwany bank stwierdził, że mimo ponownej weryfikacji sprawy, nie dała ona podstaw do zmiany jego stanowiska i odmówił zwrotu żądanej kwoty.

(dowód: wezwanie do zapłaty z dnia 15 grudnia 2017 r. wraz z potwierdzeniem nadania – k. – k. 94-95, pismo pozwanego z dnia 2 marca 2018 r. – k . 145-146)

Na stronie internetowej pozwanego banku w 2016 r. widniała informacja ostrzegawcza o zachowaniu ostrożności przy dokonywaniu bankowych czynności elektronicznych. W 2018 r. znalazły się na niej dodatkowo ostrzeżenia, że logowanie do serwisu nie wymaga podania kodu z narzędzia autoryzacyjnego. Ponadto, zamieszczono tam komunikat, żeby klient nigdy nie podawał kodu podczas logowania, ani bezpośrednio po zalogowaniu do serwisu. Jak również, żeby nie korzystać z linków do dokonania płatności przesyłanych przez osoby trzecie, a także, żeby zachować ostrożność wobec wiadomości wysyłanych np. z portali społecznościowych typu F., czy witryn ze sprzedażą typu (...), zawierających prośbę o skorzystanie z przesłanego linku w celu dokonania płatności. Linki te mogą, bowiem kierować klienta na fałszywą stronę banku.

(dowód: zrzut ekranów głównej strony logującej serwisu bankowości pozwanego – k. 144, 187)

***Sąd zważył, co następuje:***

Powództwo, jako usprawiedliwione, co do zasady, jak i co do wysokości należało uwzględnić w całości.

Na wstępie należy zauważyć, że strony łączyła umowa rachunku bankowego. Zgodnie z treścią art. 725 k.c. przez umowę rachunku bankowego bank zobowiązuje się względem posiadacza rachunku, na czas oznaczony lub nieoznaczony, do przechowywania jego środków pieniężnych oraz jeżeli umowa tak stanowi do przeprowadzania na jego zlecenie rozliczeń pieniężnych. W tym miejscu wyjaśnić należy, że zawarcie umowy rachunku bankowego powoduje, że środki pieniężne posiadacza przechodzą na własność banku. Mimo braku jednoznacznego sformułowania w odkreślonych przepisach ustawy, w doktrynie i w orzecznictwie powszechny i w zasadzie niekontrowersyjny jest pogląd, że bank uzyskuje własność deponowanych pieniędzy. Jak wskazał m.in. Sąd Apelacyjny w Krakowie w wyroku z dnia 5 lutego 2014 r., sygn.(...) (LEX nr 1540886), umowa rachunku bankowego jest oparta na konstrukcji depozytu nieprawidłowego (art. 845 k.c.), co oznacza, że bank nabywa własność wniesionych środków pieniężnych, a posiadacz rachunku bankowego nabywa roszczenie o zwrot sumy pieniężnej wynikającej z postanowień umowy łączącej klienta z bankiem. Tym samym wszelkie operacje dokonywane na rachunku bankowym wbrew woli posiadacza rachunku nie obciążają tego posiadacza, a jedynie bank. Zatem mimo wyłudzenia przez osobę nieuprawnioną mienia stanowiącego własność banku, nie dojdzie do powstania szkody po stronie posiadacza rachunku, gdyż bank nadal pozostanie zobowiązany do zaspokojenia jego wierzytelności w pełnej wysokości ze swoich środków. Ochronę wierzytelności gwarantują, bowiem posiadaczowi przepisy prawa cywilnego, finansowego i oparta na nich umowa z bankiem (zob. postanowienie Sądu Najwyższego z 28 kwietnia 2016 r., sygn. akt (...), Legalis nr 1442847).

Zgodnie z treścią art. 726 k.c. bank może obracać czasowo wolne środki pieniężne zgromadzone na rachunku bankowym z obowiązkiem ich zwrotu w całości lub w części na każde żądanie, chyba, że umowa uzależnia obowiązek zwrotu od wypowiedzenia. Wynikające z umowy uprawnienie posiadacza rachunku stanowi wierzytelność do banku

każdocześnie wymagalną, a jej rozmiary wskazuje stan konta. Z chwilą realizacji wierzytelności, przez zwrot środków pieniężnych, posiadacz rachunku odzyskuje ich posiadanie i także własność, bądź inne prawo rzeczowe lub obligacyjne, które było z nimi związane przed zdeponowaniem.

W niniejszej sprawie nie było sporne, że osoba nieuprawniona uzyskała dostęp do rachunków bankowych powodów prowadzonych przez pozwanego, o czym świadczą chociażby zgłoszenia o podejrzeniu popełniania przestępstwa złożone zarówno przez pozwanego, jak i powoda. W wyniku tego w dniach 23-26 września 2016 r. osoba ta dokonała z nich przelewów na rzecz osób trzecich. Pozwany podniósł jednak, że powodowie przyczynili się w stu procentach do powstania tejże szkody. Powyższe było spowodowane niezachowaniem przez nich należytej staranności w ochronie swoich danych, co doprowadziło do udostępnienia ich osobom nieuprawnionym, co z kolei umożliwiło wykonanie w/ w przelewów. Jak również nieposiadanie przez nich na swoim laptopie legalnego oprogramowania, w tym antywirusa spowodowało, że do systemu, którym się posługiwali przedostał się złośliwy wirus. Zarzut ten w ocenie Sądu uznać należało za niezasadny.

Stwierdzić, bowiem należy, że ryzyko dokonania wypłaty z rachunku bankowego do rąk osoby nieuprawnionej oraz dokonanie rozliczenia pieniężnego na podstawie dyspozycji wydanej przez osobę nieuprawnioną obciąża bank, także w sytuacji objęcia umowy rachunku bankowego bankowością internetową (por. wyrok Sądu Apelacyjnego w Warszawie z dnia 19 lipca 2018 r. (...), LEX nr 1822123). Podstawę odpowiedzialności banku w tym zakresie stanowią normy prawne zawarte w ustawie z dnia 19 sierpnia 2011 r. o usługach płatniczych ((...)).

Powołana ustawa o usługach płatniczych przewiduje generalną zasadę, zgodnie, z którą dostawca usług płatniczych, czyli bank, ma prawo wykonać transakcję płatniczą tylko w przypadku jej autoryzacji przez płatnika, czyli posiadacza konta. Zgodnie, bowiem z art. 46 ust. 1 powołanej ustawy, z zastrzeżeniem art. 44 ust. 2 (informacja o nieautoryzowanych transakcjach), w przypadku wystąpienia nieautoryzowanej transakcji płatniczej dostawca płatnika jest obowiązany niezwłocznie, nie później jednak niż do końca dnia roboczego następującego po dniu stwierdzenia wystąpienia nieautoryzowanej transakcji, którą został obciążony rachunek płatnika, lub po dniu otrzymania stosownego zgłoszenia, zwrócić płatnikowi kwotę nieautoryzowanej transakcji płatniczej, z wyjątkiem przypadku, gdy dostawca płatnika ma uzasadnione i należycie udokumentowane podstawy, aby podejrzewać oszustwo, i poinformuje o tym w formie pisemnej organy powołane do ścigania przestępstw. W przypadku, gdy płatnik korzysta z rachunku płatniczego, dostawca płatnika przywraca obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby nie miała miejsca nieautoryzowana transakcja płatnicza.

Przy czym zgodnie z art. 2 pkt 22 ustawy, płatnikiem jest osoba fizyczna, osoba prawna oraz jednostka organizacyjna niebędąca osobą prawną, której ustawa przyznaje zdolność prawną, składającą zlecenie płatnicze. Natomiast dostawcą płatnika jest instytucja wymieniona w art. 4 ust. 2 ustawy. Na gruncie przedmiotowej sprawy będą to odpowiednio powodowie - I. D. i P. D. oraz pozwany – (...) Bank (...) S.A. z siedzibą w W.. Jeśli natomiast chodzi o pojęcie instrumentu płatniczego to rozumie się zindywidualizowane urządzenie lub uzgodniony przez użytkownika i dostawcę zbiór procedur, wykorzystywane przez użytkownika do złożenia zlecenia płatniczego (art. 2 pkt 10 ustawy). Na gruncie przedmiotowej sprawy znaczenie ma druga cześć przedstawionej powyżej definicji, ponieważ w praktyce na pojęcie instrumentu płatniczego składa się logowanie za pomocą ustalonego wcześniej loginu klienta oraz hasła, jak również w niniejszym przypadku podania kodu numerycznego ze zdrapki oraz przepisaniu w oknie treści wyświetlanego obrazka.

W art. 45 ust. 1 cytowanej ustawy wskazano, że ciężar udowodnienia, że transakcja płatnicza była autoryzowana przez użytkownika i prawidłowo zapisana w systemie służącym do obsługi transakcji płatniczych dostawcy oraz że nie miała na nią wpływu awaria techniczna ani innego rodzaju usterka związana z usługą płatniczą świadczoną przez tego dostawcę, w tym dostawcę świadczącego usługę inicjowania transakcji płatniczej spoczywa na dostawcy tego użytkownika (ust. 1) – czyli na pozwanym (...) Banku (...) S.A. z siedzibą w W.. Przy czym wykazanie przez dostawcę zarejestrowanego użycia instrumentu płatniczego nie jest wystarczające do udowodnienia, że transakcja płatnicza została przez użytkownika autoryzowana albo, że płatnik umyślnie albo wskutek rażącego niedbalstwa doprowadził do nieautoryzowanej transakcji płatniczej albo umyślnie albo wskutek rażącego niedbalstwa dopuścił się naruszenia,

co najmniej jednego z obowiązków, o których mowa w art. 42. W drodze wyjątku od zasady określonej w art. 6 k.c., ciężar udowodnienia tychże trzech okoliczności zgodnie z ust. 2 powołanego przepisu ciąży na dostawcy.

Po pierwsze, bank może uwolnić się od obowiązku niezwłocznego zwrotu kwoty transakcji w przypadku wykazania, iż to osoba uprawniona do wykonywania operacji na tym rachunku była osobą, która dokonała autoryzacji. Zgodnie z art. 40 ust. 1 ustawy, transakcję płatniczą uważa się za autoryzowaną, jeżeli płatnik wyraził zgodę na wykonanie transakcji płatniczej w sposób przewidziany w umowie między płatnikiem a jego dostawcą. W § 2 pkt 2 regulaminu świadczenia usług bankowości elektronicznej w (...) Banku (...) S.A. z siedzibą w W. wskazano natomiast, że autoryzacja transakcji płatniczej przez płatnika to złożenie dyspozycji, w tym zgoda na jej wykonanie w elektronicznych kanałach dostępu poprzedzone weryfikacją klienta lub użytkownika, jeśli jest on ustanowiony (w niniejszej sprawie nie był ustanowiony). Strony postępowania zgodnie potwierdziły, że sposobem autoryzacji wszystkich operacji na rachunku powodów była karta kodów jednorazowych, czyli kodów numerycznych z tzw. „zdrapki". Powyższe wyraźnie, zatem wskazuje, że jeżeli transakcja płatnicza jest autoryzowana, oznacza to, że zgodę na transakcję wyraził sam płatnik - tutaj - P. D., bowiem to on usługiwał konto internatowe powodów. Nie jest, więc autoryzowaną taka transakcja, której dokonano przy użyciu instrumentu płatniczego należącego do płatnika i dokonano uwierzytelnienia, ale proces ten został dokonany bez zgody płatnika, np. poprzez kradzież przez osobę trzecią niezbędnych danych ku tejże autoryzacji.

Na gruncie przedmiotowej sprawy, w ocenie Sądu, brak jest podstaw do stwierdzenia, że I. D. i P. D. wyrazili zgodę na wykonanie przelewów w dniach 23-26 września 2016 r. na łączną kwotę 112.137 zł. Powodowie stanowczo temu zaprzeczali, a sam pozwany nie kwestionował tej okoliczności, tym bardziej, że sam zgłosił zawiadomienie o podejrzeniu popełniania przestępstwa na rachunku powodów przez cyberprzestępców. Podkreślić jednak należy, że transakcje w w/w dniach były uwierzytelnione, ponieważ osoba nieuprawniona – hacker, użyła wyłudzonych od małżonków D. instrumentów, które miały identyfikować posiadacza rachunku bankowego, tj. login i hasło oraz jednorazowy kod numeryczny z tzw. „zdrapki". Mimo to transakcje nie zostały autoryzowane przez powodów, ponieważ powód, który zajmował się bankowością elektroniczną, – co przyznała powódka, a nie zaprzeczył pozwany – sam ich nie autoryzował. Co warto zaznaczyć, system bankowy pozwanego wykrył część działań powodów, albowiem ja to wynika z zeznań świadka P. C. – wykrył szybkie przelewy (...) wykonywane na rachunku powodów przez osoby trzecie i je zablokował. Świadek ten natomiast nie potrafił wyjaśnić przed Sądem, dlaczego bank nie zawiesił przelewów zwykłych – ELIKSIR, skoro przelewy SORBET zostały zablokowane (k. 206 v). Mając na uwadze powyższe, uznać zatem należy, że transakcje przeprowadzone na koncie I. D. i P. D. w dniach 23-26 września 2016 r. nie były przez nich autoryzowane.

Przechodząc do kolejnych przesłanek, których udowodnienie zwolniłoby pozwany bank z odpowiedzialności, podkreślić należy, że pozwany nie udowodnił, że powodowie, jako płatnicy umyślnie doprowadzili do nieautoryzowanej transakcji płatniczej, albo umyślnie lub wskutek rażącego niedbalstwa dopuścił się naruszenia, co najmniej jednego z obowiązków, o których mowa w art. 42 ustawy.

Należy wskazać, że zgodnie z art. 46 ust. 3 ustawy o usługach płatniczych, płatnik, (czyli w tym wypadku powodowie) odpowiada za nieautoryzowane transakcje płatnicze w pełnej wysokości, jeżeli doprowadził do nich umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia, co najmniej jednego z obowiązków, o których mowa w art. 42. Generalnie przepis art. 46 ustawy o usługach płatniczych – który cytowany był na wstępnie - jest przepisem szczególnym, regulującym odpowiedzialność banku w przypadku wystąpienia nieautoryzowanej transakcji płatniczej. Odpowiedzialność banku za taką transakcję jest uchylona w razie doprowadzenia do nieautoryzowanej transakcji przez klienta w sposób umyślny lub wskutek umyślnego albo stanowiącego rażące niedbalstwo naruszenia obowiązków, o których mowa w art. 42.

Podkreślić należy, że naruszenie obowiązków z art. 42 ustawy musi nastąpić umyślnie lub w skutek rażącego niedbalstwa. O winie płatnika można mówić wówczas, gdy zaistniałe zdarzenie, (czyli wystąpienie nieautoryzowanych transakcji) nastąpiło wskutek okoliczności, za które ponosi on odpowiedzialność. W orzecznictwie Sądu Najwyższego ukształtował się pogląd, że „rażące niedbalstwo to coś więcej niż brak zachowania zwykłej staranności w działaniu.

Chodzi tu o takie zachowanie, które graniczy z umyślnością" (wyrok Sądu Najwyższego z dnia 29 stycznia 2008 r., sygn. (...), LEX nr 1620328).

Zgodnie z art. 42 ust. 1 ustawy o usługach płatniczych, użytkownik uprawniony do korzystania z instrumentu płatniczego jest obowiązany: 1) korzystać z instrumentu płatniczego zgodnie z umową ramową oraz 2) zgłaszać niezwłocznie dostawcy lub podmiotowi wskazanemu przez dostawcę stwierdzenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu. W celu spełnienia obowiązku, o którym mowa w ust. 1 pkt 1, użytkownik, z chwilą otrzymania instrumentu płatniczego, podejmuje niezbędne środki służące zapobieżeniu naruszeniu indywidualnych danych uwierzytelniających, w szczególności jest obowiązany do przechowywania instrumentu płatniczego z zachowaniem należytej staranności oraz nieudostępniania go osobom nieuprawnionym (ust. 2).

Zasygnalizować ponownie należy, że nieautoryzowane operacje płatnicze zostały wykonane w dniach 23-26 września 2016 r., a system bankowy pozwanego wówczas nie wykrył części nieprawidłowości w zakresie użycia instrumentu płatniczego. Nieznana osoba korzystając z wykradzionych przez siebie danych logowania oraz nr kodu wykonała przelewy zewnętrzne bez wiedzy i zgody powodów. Kluczowym dla kwestii zasadności przedmiotowego powództwa jest, więc stwierdzenie czy uzyskanie danych do logowania do sytemu bankowego oraz uzyskanie przez nieznaną osobę kodu weryfikacyjnego wynikało z rażącego niedbalstwa P. D..

Zdaniem Sądu, powodowi, – bo tylko on zajmował się internatową bankowością małżonków D. – nie można przypisać umożliwienia dokonania nieautoryzowanych transakcji umyślnie, jak również wskutek rażącego niedbalstwa.

Podkreślić należy, że przede wszystkim brak było w sprawie dowodów o przekazaniu podczas zawierania przez małżonków D. umowy jakichkolwiek informacji o sprzęcie za pomocą, którego mogli dokonywać operacji bankowych, w tym sposobie jego zabezpieczenia, konserwacji oraz potencjalnych zagrożeń tj. ataki hackerskie. Pozwany, co prawda próbował dowodzić, że informacja ostrzegawcza o zachowaniu ostrożności przy dokonywaniu bankowych czynności elektronicznych, widniała na jego stronie internetowej już w chwili dokonywania transakcji handlowych przez powodów, jednak w ocenie Sadu było to nieskuteczne. Niewątpliwie powód, podczas logowań od 2010 r., – kiedy to zaczął korzystać z usług bankowości internetowej, był zawsze ostrożny – w końcu przez 6 lat, nic się złego nie działo, a on sam był zadowolony z tej formy operacji bakowych. Sam, podczas zeznań wskazywał, że każdorazowo zwracał uwagę na stronię internetową banku i jej zabezpieczenia – wyposażenie w zieloną kłódkę i prefiks witryny „https", czego pozwany nie kwestionował. Pozwany nie wykazał aby inne, szczegółowe informacje o zagrożeniach były umieszczone na stronie banku w dniu zdarzenia hackerskiego na konto powoda. Chodzi tu o ostrzeżenia:

- że logowanie do serwisu nie wymaga podania kodu z narzędzia autoryzacyjnego,

- aby klient nigdy nie podawał kodu podczas logowania, ani bezpośrednio po zalogowaniu do serwisu,

- żeby nie korzystać z linków do dokonania płatności przesyłanych przez osoby trzecie,

- żeby zachować ostrożność wobec wiadomości wysyłanych np. z portali społecznościowych, czy witryn ze sprzedażą, zawierających prośbę o skorzystanie z przesłanego linku w celu dokonania płatności.

Z dużą dozą prawdopodobieństwa należy stwierdzić, że takie informacje – ostrzeżenia, pojawiają się na stronach różnych banków, po każdym „nowym" ataku cyberprzestępców na ich klientów. Banki – mimo szeregu specjalistów – nie są w stanie przewidzieć wszystkich możliwych sposobów wyprowadzenia pieniędzy z rachunków swoich klientów. Jeśli natomiast się one pojawią, (czyli konto jakiegoś klienta zostanie już zainfekowane) dopiero aktualizują i rozszerzają informacje ostrzegawcze w tym zakresie. Pozwany Bank wykazał, że informacje te znajdują się obecnie na witrynie banku. Z tego faktu nie można jednak wywodzić wcześniejszej odpowiedzialności powodów za zagrożenia o których nie mieli pojęcia.

Kolejno trzeba wskazać, że wchodząc na stronę internetową pozwanego banku w dniu 22 września 2016 r., była ona bliźniacza, jak ta prawdziwa. Jej szata graficzna i pojawiające się informacje nie wzbudziły u powoda żadnej niepewności, albowiem były identyczne jak te pojawiające się do tej pory, czyli przez prawie 6 lat od czasu korzystania z bankowości elektronicznej przez powoda. W tym miejscu, zatem należy przytoczyć treść § 10 regulaminu świadczenia usług bankowości elektronicznej w (...) Banku (...) S.A. z siedzibą w W., który stanowi, że świadczenia usług bankowości elektronicznej pozwanego obowiązujących powodów, wskazuje, że klient mógł składać dyspozycje za pośrednictwem elektronicznych kanałów dostępu przez całą dobę z wyłączeniem okresu przerw niezbędnych do konserwacji, napraw technicznych lub przywrócenia poprawności funkcjonowania elektronicznych kanałów dostępu. Informacje o wystąpieniu przerwy są dostępne na stronie internetowej lub w serwisie internetowym lub serwisie telefonicznym. W ocenie Sądu, biorąc pod uwagę treść powyższego paragrafu, powód miał, zatem prawo pozostawać w usprawiedliwionym przekonaniu, że komunikat wyświetlający się podczas logowania jest prawdziwy i pochodzi właśnie od pozwanego banku.

Jeśli zaś chodzi o zainstalowanie oprogramowania antywirusowego na laptopie powoda, to należy wskazać, że obecnie nie jest to do udowodnienia. Tak samo jak to czy komputer został zawirusowany złośliwym oprogramowaniem lub oprogramowaniem wyłudzającym dane. Jak również czy ewentualnie po zainstalowaniu wirus przedostał się do komputera powoda z chwilą odbioru przez niego maila o dostarczeniu mu przez kuriera paczki. Zgodnie, bowiem, z przebiegiem rozmów powoda z pracownikiem banku – po tzw. „rozeznaniu się przez niego w sytuacji" - polecono mu dokonać reinstalacji systemu operacyjnego, co powód uczynił za pośrednictwem serwisu komputerowego. Powyższe ustalono, na podstawie nagrań CD z tychże rozmów. Natomiast niemożność weryfikacji danych znajdujących się w dniu zdarzenia na laptopie powoda ustalono na podstawie opinii biegłego sądowego, który de facto przebadał również ten laptop już w toku postępowania przygotowawczego. W ocenie Sądu opinia ta była rzetelna i konkretna. Zawierała odpowiedzi na wszystkie postawione przez Sąd, a jednocześnie przez strony postępowania pytania. Również po wytłumaczeniu bardziej skomplikowanych kwestii języka informatycznego bezpośrednio przez Sądem na rozprawie, żadna ze stron postępowania jej nie kwestionowała.

W ocenie Sądu, zatem, wpisanie przez powoda kodu ze zdrapki po zalogowaniu się do swojego konta, kiedy ten był już pewny, że znajduje się na właściwej stronie banku, nie nosi cech rażącego niedbalstwa. Natomiast to działanie pracowników powoda należy uznać za nieprawidłowe, albowiem przez nich obecnie, tj. w niniejszym postępowaniu nie da się zweryfikować oraz udowodnić w/w kwestii podanych w poprzednim akapicie.

Będąc już w kwestii zagadnień informatycznych, to odnieść się należy do złożonego na ostatniej rozprawie przez pozwanego wniosku o przeprowadzenie dowodu z opinii biegłego na okoliczność ustalenia adresu IP komputera powoda. W ocenie Sądu wniosek ten należało pominąć, albowiem po pierwsze okoliczności, na które został powołany zostały już dostatecznie wyjaśnione, a ponadto wobec treści opinii biegłego, nie miał już znaczenia dla rozpoznania niniejszej sprawy. Jak podał biegły w ustnej opinii - adres IP wskazywał, że transakcje na koncie bankowym powodów wykonano z tego samego komputera. Powodem tego mogły być dwie sytuacje - albo obie operacje zostały dokonane przez cyberprzestępcę albo są działaniem bardzo złożonego wirusa. Tym bardziej wbrew hipotetycznym twierdzeniom pozwanego, nie mogli tego dokonać powodowie. Tym niemniej należy wskazać, że to przede wszystkim na banku, jako profesjonalnym podmiocie ciążyły ustawowe obowiązki wskazane m.in. w art. 43 ust. 1 ustawy o usługach płatniczych. Ponadto zobowiązanie banku względem posiadacza rachunku kształtuje również przepis art. 50 ust. 2 ustawy z 29 sierpnia 1997 r. - Prawo bankowe (tekst jedn.: (...)), który stanowi, iż bank jest zobowiązany do dołożenia szczególnej staranności w zakresie zapewnienia bezpieczeństwa przechowywanych środków pieniężnych. Brak wytłumaczenia ze strony pozwanego, dlaczego część działań cyberprzestępców została przez jego instrumenty wychwycona, a część nie, nie może w żadnym razie działać na jego korzyść. Tak samo jak niepoinformowanie – mimo kilkunastu rozmów telefonicznych pracowników banku z powodem o zaborze jego środków oraz udzielenie mu porady skutkującej zatarciem dowodów, stawia go zdaniem Sądu w niewątpliwym negatywnym świetle.

Powód, zatem w ocenie Sądu nie naruszył, obowiązku wskazanego w art. 42 ust. 1 pkt 1 i ust. 2 ustawy o usługach płatniczych.

Drugim z obowiązków określonych w art. 42, którego naruszenie w sposób określony w art. 45 ust. 2 pkt 2 powodowałoby uchylenie odpowiedzialności banku, polega na niezwłocznym zgłoszeniu dostawcy lub podmiotowi wskazanemu przez dostawcę stwierdzenia utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu. Podkreślić należy, że powód nie mógł niezwłocznie podać takiej informacji bankowi, skoro zaufał informacjom podanym na stronie internetowej banku, że jest ona w przebudowie. Powyższe nie wskazywało niczego niepokojącego. Następnie przez kilka dni nie korzystał z bankowości internetowej, ponieważ nie miał takiej potrzeby, zaś kolejno był poza domem – na weselu. Z ustalonego stanu faktycznego wynika, że jako pierwszy o nieuprawnionym użyciu instrumentu płatniczego dowiedział się sam pozwany. Mimo czterokrotnych rozmów z powodem, żaden z jego pracowników, nie powiedział mu wprost, że jego środki pieniężne, zostały wytransferowane na zewnątrz przez osobę trzecią, mimo, że pracownicy już podczas rozmowy posiadali tę wiedzę. Jedynie – jak wskazano wyżej - polecono mu wykonać „czyszczenie" laptopa, w którym mogą znajdować się wirusy. Natomiast sam bank zgłosił zawiadomienie o możliwości popełnienia przestępstwa, tj. bezprawnego wydobycia środków pieniężnych z konta powodów. Skoro pozwany pierwszy powziął powyższą wiedzę, zaś powód – mimo możliwości przekazania mu tej informacji – nie wiedział o niej, był on zwolniony z obowiązku zawiadomienia banku, wskazanego z powołanym przepisie.

W niniejszej sprawie nie znajduje, zatem zastosowania art. 46 ust. 3 ustawy o usługach płatniczych, gdyż powodowie nie naruszyli obowiązków, o których mowa w art. 42 ustawy. Bezzasadne jest tym samym twierdzenie pozwanego, że powodowie, a dokładniej powód przyczynił się do utraty ich środków pieniężnych z ich rachunku bankowego.

Mając na uwadze poczynione powyżej ustalenia, należy wskazać, że pozwany w żaden sposób nie wykazał zaistnienia którejkolwiek z przesłanek wyłączających jego odpowiedzialność w niniejszej sprawie. Nie ulega wątpliwości, że powodowie nie autoryzowali przelewów z dni 23-26 września 2016 r., nie doprowadzili umyślnie do nieautoryzowanych transakcji płatniczych, ani nie dopuścili się do rażącego naruszenia obowiązków z art. 42 ust. 1 ustawy, gdyż dane potrzebne do logowania i wykonania przelewu zostały od powoda uzyskane podstępnie przez podmiot nieuprawniony. W związku z tym, bank był zobowiązany do niezwłocznego przywrócenia obciążonego rachunku płatniczego do stanu, jaki istniałby, gdyby nie miały miejsca nieautoryzowane transakcje płatnicze, czego nie uczynił.

W związku z powyższym, zgodnie z art. 46 ust. 1 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych ((...)), pozwany jest zobowiązany niezwłocznie zwrócić powodom kwotę nieautoryzowanych transakcji płatniczych, która wyniosła 97.210 zł (bez kwoty zwróconej im w toku postępowania przygotowawczego), o czym orzeczono w pkt I sentencji wyroku.

W zakresie żądania zasądzenia odsetek, Sąd orzekł na podstawie art. 481 § 1 k.c., zgodnie, z którym, jeżeli dłużnik opóźnia się ze spełnieniem świadczenia pieniężnego, wierzyciel może żądać odsetek za czas opóźnienia, chociażby nie poniósł żadnej szkody i chociażby opóźnienie było następstwem okoliczności, za które dłużnik odpowiedzialności nie ponosi. Zgodnie z art. 46 ust. 1 ustawy o usługach płatniczych, pozwany miał obowiązek niezwłocznego zwrotu kwoty nieautoryzowanych transakcji. Przyjmuje się, że termin „niezwłocznie" oznacza termin realny, mający na względzie okoliczności miejsca i czasu. Mając na uwadze okoliczność, że bank sam w okresie 23-26 września 2016 r. dokonał blokady przelewów sorbnetowych, to już wówczas wiedział o nieprawidłowościach dokonywanych na rachunkach powodów. Zatem roszczenie odsetkowe zasługuje na uwzględnienie od daty żądanej w pozwie, czyli od dnia 26 września 2016 r.

Mając na uwadze powyższe rozważania faktyczne i prawne, Sąd uznał powództwo za zasadne w całości.

Sąd orzekł o kosztach procesu orzekł w pkt II sentencji wyroku na podstawie art. 98 § 1, 3, 4 k.p.c. w zw. z art. 99 k.p.c., zasądzając od pozwanego solidarnie na rzecz powodów kwotę 6.417 zł stanowiącą koszty poniesione przez nich w toku procesu, na które złożyły się: 1.000 zł - opłata sądowa od pozwu, 5.417 zł - wynagrodzenie pełnomocnika, które to ustalone zostało na podstawie § 2 ust. 6 rozporządzenia Ministra Sprawiedliwości z dnia 22 października 2015 r. w sprawie opłat za czynności radców prawnych ((...)) oraz 17 zł – opłata skarbowa od pełnomocnictwa.

Zarządzeniem z dnia 21 grudnia 2018 r. na podstawie art. 80 u.k.s.c. po uprawomocnieniu się wyroku nakazano zwrócić powodom kwotę 3.861 zł tytułem nadpłaconej opłaty sądowej od pozwu.

# ZARZĄDZENIE

1. odnotować,

2. doręczyć pełnomocnikowi pozwanego,

3. przedstawić wraz z apelacją lub po upływie 14 dn.

O., dnia 14 stycznia 2019 r.